Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1702 01/09/15

~ Sony Hackers Got Sloppy ~ People Are Talking! ~ Classic Video Games!
~ FCC on Net Neutrality! ~ New Bitcoin Loss Claim ~ MIT Sites Defaced!
~ Win 8.1 Vulnerability! ~ US Did Not Hack Back! ~ Macro-based Malware!

~ Protecting Free Speech! ~ ~ Facebook Adults: 58%

-* Anticipated Games for 2015! *-
-* Hacking Group Publishes Xbox One SDK *-
-* Strange Resurrection of Atari’s Buried ET! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Is there any "good" news in the world these days?? It seems like everything being seen on television or in the newspaper is negative and/or morbid! Our thoughts these days go out to publication of Charlie Hebdo, where 12 people were executed by terrorists this past week. More atrocities carried out by self-proclaimed religious zealots! The nut cases are trying to take control of the world - truly not something really new, is it?

How have you all been faring lately with this weather? For the first time in a number of years, we woke up here one morning this week to temperatures in the negative numbers! And, add in the wind gusts, we were feeling it in the double-digits!

So, while we do whatever we can here to stay warm, we hope you curl up somewhere comfortable and take a gander at this week’s issue!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - The Strange Resurrection of Atari’s Long-Buried E.T.!
"""""""""""""""""""""""""""""""""

Most Anticipated Video Games for 2015!
Hacking Group Publishes Xbox One SDK!
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""""

Legend of Zelda, Batman: Arkham Knight Among Anticipated Video Games for 2015

Link, Master Chief, Batman and Nathan Drake will be back in action.

The leading men are among the protagonists starring in totally new video game instalments in 2015, joined by newcomers like a team of intergalactic monster hunters and their prey (Evolve), a band of high-tech criminals and their tails (Battlefield Hardline) and a battalion of explorers and their procedurally generated universe (No Man's Sky).

The gaming line-up for 2015 also includes a pair of original Victorian-inspired tales (Bloodborne, The Order: 1886), the return of two long-gone, out-of-this-world gaming franchises (Star Wars: Battlefront, Star Fox and an expedition into the open-world genre for a long-running stealth series (Metal Gear Solid V: The Phantom Pain).

Here's a glimpse of some of 2015's most anticipated games:

Batman: Arkham Knight: After three editions of stomping, gliding and grappling through a virtual Gotham, Batman has keys to the Batmobile in Rocksteady Studios' Dark Knight finale. This time, besides old-school baddies like Penguin and Scarecrow, Batman is facing off against a new menace called the Arkham Knight. (for PlayStation 4, Xbox One, PC; June 2)

Promotional trailers for Battlefield: Hardline were criticised for its bombastic version of cops versus robbers in light of the recent protests against police violence in the U.S. (Electronic Arts/Associated Press)

Battlefield Hardline: Visceral Games is dodging the military in favour of an interactive game of cops and robbers in the latest entry of the first-person Battlefield shooter series. The war-on-crime action will include bank heists, police chases and hostage rescue missions. (for PlayStation 3, PlayStation 4, Xbox 360, Xbox One, PC; March 17)

Bloodborne: Dark Souls mastermind Hidetaka Miyazaki takes a stab at the PlayStation 4 with this relentless role-playing title set in a gothic enclave that's been overrun by infected monsters. Bloodborne, much like predecessors Dark Souls and Demon's Souls, is expected to be quite the nightmare. (for PlayStation 4; March 24)

Evolve: After tackling team-based zombie slaying with Left 4 Dead, Turtle Rock Studios takes on monster hunting in this multiplayer shooter with a twist. Instead of equal squads aiming for each other online, Evolve pits a team of four against one player portraying an oversized, overpowered behemoth. (for PlayStation 4, Xbox One, PC; Feb. 10)

Halo 5: Guardians: (for Xbox One, fall 2015): For his latest interstellar adventure, hardened "Halo" hero Master Chief is joined by a new companion, fellow supersoldier Locke. Developer 343 Industries has injected a slew of fresh abilities into the game's multiplayer mode, including thruster-boosted dodging and ground pounding.

Microsoft hopes to correct the underwhelming response to Halo: Master Chief Collection with the brand-new Halo 5: Guardians. (Microsoft/Associated Press)

The Legend of Zelda: Link and his trusty steed Epona are set free in an expansive open realm in the first original Legend of Zelda adventure crafted for Nintendo's high-definition, touchscreen-centric Wii U

console. Legend of Zelda producer Eiji Aonuma has promised that Link's actions will have the ability to reshape his fantasy world. (for Wii U, 2015)

Metal Gear Solid V: The Phantom Pain: Metal Gear's one-man army Snake is dispatched to Afghanistan during the Cold War to take down Soviet forces. Phantom Pain seeks to be the most liberating Metal Gear, yet with sandstorms and daylight affecting the mercenary's stealthy tasks. (for PlayStation 3, PlayStation 4, Xbox 360, Xbox One, PC; 2015)

No Man's Sky: While most game makers precisely position every polygon within their creations, the developers at Hello Games are dispatching players to virtual worlds with randomly generated landscapes, meaning plants, animals and atmospheres will look different for each person who picks up this ambitious exploration title. (for PlayStation 4, PC, 2015)

No Man's Sky, by British indie studio Hello Games, promises an entire galaxy to explore and discover. (Hello Games)

The Order: 1886: In this third-person alternate history romp, the Knights of the Round Table battle supernatural forces with steampunk gear across London. The Order creators Ready at Dawn are harnessing the PS4's souped-up processing power to transport gamers to an intricate and moody rendition of the foggy city. (for PlayStation 4, Feb. 20)

Uncharted 4: A Thief's End: After surviving a trek through a sprawling desert and a jaunt through an ancient crumbling city, Uncharted champion Nathan Drake returns for his first quest on the PS4. This time, the smart-alecky treasure hunter will be joined by his brother, portrayed by omnipresent video game actor Troy Baker. (for PlayStation 4; 2015)

Other anticipated titles include: role-playing sequel The Witcher 3: Wild Hunt; online-only shooter Tom Clancy's The Division; time-bending action title Quantum Break; a next-gen rendition of Star Wars: Battlefront; Lara Croft follow-up Rise of the Tomb Raider and Star Fox for the Wii U.

Hacking Group Publishes Xbox One SDK, Threatens To Leak Unreleased Game Builds

Following Lizard Squad's takedown of the Xbox One network over Christmas, Microsoft's festive woes continue after another hacking group managed to get hold of and subsequently release the November 2014 Xbox One software development kit (SDK).

The group, which calls itself @notHALT on Twitter but which some news outlets are referring to as H4LT, uploaded the kit and its associated documentation to file sharing site Mega.

Hey, @Xbox! We thought we'd drop on by and End 2014 with a Bang ;)

Budding bedroom coders will not of course not be able to release their own programs officially developers must register and be approved before posting games to Xbox's release channels but @notHALT is hoping that leaking the SDK could potentially lead to homebrew applications in the future.

Speaking to the SevenSins website, via Direct Message on Twitter, @notHALT

said:

Once the SDK is out, people who have knowledge or has in the past reversed files related to the Windows (8) operating system should definitely have a go at reversing some files in there. Why? Well, the Xbox One is practically a stripped Windows 8 device and has introduced a new package format that hasn’t had much attention. This format is responsible for updating the console and storing applications (Games are under the category of ’Applications’ on the Xbox One) and is a modification of Virtual Hard Disks. There is no definite ’exploit’ but from what we have studied and tested, this simple packaging format could possibly lead us to creating Homebrew applications for the Xbox One.

In a separate conversation with The Independent newspaper, @notHALT also claimed to have gained access to a new cloud-based system used by developers to store early versions of their new games, including Microsoft-owned 343 Industries’ Halo 5 which is yet to receive a firm release date.

The account that was compromised is not thought to belong to 343 Industries but the hackers say it did give them access to files uploaded by that company.

@notHALT told The Independent that it hopes to leak the additional files after speaking with Lizard Squad who it hopes can help with "protection and stress testing of its systems for when the rest of the data is leaked".

According to @notHALT, none of its members know anyone within the Lizard Squad personally but they are in contact with each other.

Internet Archive Offers 2,300+ Classic Video Games To Play Online for Free

Load up your wagon, buy your provisions and hit The Oregon Trail it’s like the ’80s all over again.

The Internet Archive, the people who brought us The Wayback Machine, has made more than 2,300 old let’s say classic - MS-DOS games available to play via streaming. The archive has been working since 2013 to store and host these video games.

There’s our favorite, "The Oregon Trail" (the original and deluxe), but there’s also "SimCity," "Prince of Persia" and "Where in the World is Carmen Sandiego?" (which, btw, turns 30 this year) among many, many others.

Jason Scott, longtime curator at the archive, warns that playing might not be everything you remember - some of the games "will still fall over and die, and many of them might be weird to play in a browser window."

Scott is also asking gamers to try out the archive’s new beta design.

So get out there on the Oregon Trail, but be careful: I got cholera 26 miles down the trail.

More Than 2,000 Classic MS-DOS Games Now Available in Your Browser for Free

The Internet Archive exists to preserve a library of digital content just as a brick-and-mortar library or a museum preserves physical items that are culturally significant. And games of course fall into that category. Ask any gamer what was the first game he played, or the first game he fell in love with, and sit back and prepare for the passion.

Now gamers older and younger alike can access some of the most iconic older MS-DOS titles for free, thanks to the Internet Archive s efforts (2015 is off to a productive start). At the time of writing, the organization had collected some 2,314 old MS-DOS games games that are no longer playable on current platforms, and therefore might be considered abandonware and made them available for free on its website.

Titles include 1990 s Prince of Persia, 1990 s The Oregon Trail, 1997 s Bust-A-Move, 1992 s Wolfenstein 3D, the original Metal Gear from 1990, 1987 s Maniac Mansion, 1989 s Sim City and even a fan-made update of 1986 s original The Legend of Zelda.

The games are playable using a browser-based emulator created by the Internet Archive for this specific purpose, EM-DOSBOX. It s still in beta, which means it may occasionally experience a bug here and there; and, of course, there are no manuals accompanying the titles, so you may have to rely on trial and error to figure out how to play.

You can check it out for yourself on the Internet Archive website (https://archive.org/details/softwarelibrary_msdos_games/v2).

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

The Strange Resurrection of Atari’s Long-Buried E.T.

The National Museum of American History, part of the Smithsonian, has added a vintage copy of the Atari 2600 video game E.T. the Extra-Terrestrial to its collection. This particular game is meant to fill a void in the museum’s collection, namely the unrepresented dark days of the 1980s when the United State video game industry crashed.

This Atari game didn’t come from an old collection, though. Rather, it’s an example of the truism that one person’s trash is another’s treasure. Many museums around the world feature pieces of art that were recovered at archeological dig sites, but this game cartridge was unearthed at a New Mexican landfill.

Atari helped launch the home video game console market in the late 1970s. By 1982, the company faced intense competition from the likes of Mattel’s Intellivision and Coleco’s Colecovision. At the same time, a slew of

independent game developers, hoping to cash in on the install bases of those consoles, began to flood the market with lackluster titles.

The market already was poised for a crash when Atari made the rash decision to rush out a game tied to Warner Bros.' hit film E.T. the Extra-Terrestrial. Atari, which reportedly spent between US$20 million and $25 million for the rights to the Steven Spielberg film, commissioned a game title to be produced within six weeks at a time when game development typically took six to nine months. It needed to sell 4 million copies for the title to be a success.

"That is a lot to pin on one game," said video game industry consultant P.J. McNealy.

Atari had set itself up for disaster - it shipped fewer than a million copies.

Still, it is "worth remembering that this is one of the first - if not the first - big movie tie-ins for games," McNealy told TechNewsWorld. "The game didn't sell, but it is really a broad stroke. This is part of the correlation not causation" of the industry's decline.

Since the E.T. games weren't selling at stores, and many that did sell subsequently were returned, Atari made another rash decision and buried some of the unsold games in a landfill in Alamogordo, New Mexico. To deter people from seeking out the games, Atari claimed they had been covered by concrete. The company kept their exact location secret.

For more than 30 years, rumors about the location of the site circulated, and the intense speculation gradually transformed into an urban legend.

Last year, Alamogordo's city council voted to allow gaming company Fuel Industries to search for the games, and the site was discovered. Dozens of copies were found, and one was supplied to Smithsonian museum technician Drew Robarge.

The cartridge and what is left of its packaging have been added to the permanent collection of The National Museum of American History.

"Despite it being a dreadful game, E.T. represents something more substantial than bad design," said Jon Gibson, cocurator of Iam8Bit.

"It's a symbol of the game industry's ambition," he told TechNewsWorld. "They manufactured more E.T. cartridges then there were Atari consoles to play them on. E.T. is a relic of impossible, hilarious ego."

Atari's E.T. is just one aspect of a much larger problem that developed during the early days of the game console industry.

"That game has become a symbol of the domestic crash in the video market that occurred between 1983 and 1985," said Lewis Ward, IDC research director for gaming.

"Ascribing a multiyear crash like that to a single game is of course a misleading oversimplification of what happened," he told TechNewsWorld.

"Still, the symbol stuck, and the strange details of the saga - such as the fact that millions of copies of the game were buried in New Mexico, like some reverse Roswell - helps to keep the story alive," Ward noted.

"Contrasting the massive hit that was E.T. the movie and the massive flop of the Atari game tie-in is another memorable juxtaposition," he observed. "The video game industry was in its infancy in the early ’80s. Volatility is normal in such a young market."

Because the video game industry is just a few decades old, it is somewhat ironic that one of its historic artifacts was recovered through a type of archeology. The Smithsonian no doubt sees the tongue-in-cheek value of pulling an historic flop from the muck and preserving it for posterity.

"From the Smithsonian’s perspective, this is a bid to stay relevant among millennials. They’re trying to augment their collection of material that relates to fairly recent cultural developments," said Ward.

"Gaming tends to be much more popular among youths and younger adults, so by adding this type of content it may help drive the next generation of Americans through the turnstiles," he added.

"There are now four generations of gamers," McNealy noted. "The Smithsonian is finally taking notice of an exciting time for the industry - even if it was a dark one. Gaming is finally getting its historical due."

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

FBI Says Sony Hackers ’Got Sloppy,’ Posted from North Korea Addresses

FBI Director James Comey said on Wednesday that hackers behind the cyberattack on Sony Pictures Entertainment provided key clues to their identity by sometimes posting material from IP addresses used exclusively by the North Korean government.

The hackers, who called themselves "Guardians of Peace," sometimes "got sloppy" and failed to use proxy servers that would hide their identity, Comey said at the International Conference on Cyber Security in New York.

"The Guardians of Peace would send emails threatening Sony employees and post online various statements explaining their work. In nearly every case they would use proxy servers in sending those emails and posting those statements," Comey said.

"But several times they got sloppy. Several times, either because they forgot or they had a technical problem, they connected directly and we could see it," Comey said.

"We could see that the IP addresses they used ... were IPs that were exclusively used by the North Koreans. It was a mistake by them. It was a very clear indication of who was doing this. They would shut it off very quickly once they realized the mistake, but not before we saw them

and knew where it was coming from," he added.

Sony’s network was crippled by hackers in November as the company prepared to release "The Interview," a comedy about a fictional plot to assassinate North Korean leader Kim Jong Un. The attack was followed by online leaks of unreleased movies and emails that caused embarrassment to executives and Hollywood personalities.

Comey urged the U.S. intelligence community to declassify information that showed the hackers used such servers. Critics of the FBI and spy agencies have accused the government of failing to back up assertions that North Korea was responsible.

Comey said investigators still do not know how hackers got into Sony’s systems. But he said technical analysis of the malware used showed strong similarities to malware developed by North Korea and used last year in attacks on South Korean banks.

He said language used by Guardians of Peace also matches language used in other hack attacks attributed to North Korea.

Comey said the FBI would deploy more cybersecurity experts to work in the offices of its foreign partners in order to "shrink the world" the way hackers have done.
U.S. officials familiar with investigations into the attack say while U.S. agencies believe North Korea initiated it, they are also looking into whether Pyongyang hired outside help.

One of the officials said investigators believe the North Koreans could either have hired foreign hackers to help with the attack or got help from disgruntled Sony insiders. They do not believe North Korea had help from any other government.

Speaking before Comey at the cyber conference, James Clapper, the U.S. Director of National Intelligence, said the Sony hack was the most serious cyberattack ever targeting U.S. interests.

Clapper said cyberattacks offered the North Koreans "global recognition at a low cost with no consequences."

He added that he had watched "The Interview" over the past weekend. "It’s very clear to me that the North Koreans don’t have a sense of humor," he said.

US Did Not ’Hack Back’ Against North Korea

The U.S. government was not responsible for sustained electronic attacks that crippled North Korea’s Internet infrastructure last month, just after President Barack Obama promised that his administration would respond to the hacker break-in at Sony Pictures Entertainment Inc., two senior U.S. officials told The Associated Press.

The Obama administration has been deliberately coy about whether it caused North Korea’s outage, which affected all the nation’s Internet connections starting the weekend of Dec. 20. But the two officials, speaking on condition of anonymity because they were not authorized to openly discuss the issue, acknowledged to the AP that it was not a U.S.

operation.

It was not immediately clear even within the administration whether rogue hackers or other governments disrupted North Korea’s networks. The networks are not considered especially robust since they rely on a single provider, China United Network Communications Group Co. Ltd., the state-owned provider in neighboring China. North Korea’s service was sporadic starting Saturday, Dec. 20, then collapsed entirely for nearly 10 hours two days later in what has remained an enduring whodunit.

"It looks more like the result of an infrastructure attack than an infrastructure failure," said James Cowie, chief scientist at Dynamic Network Services Inc. of Manchester, New Hampshire, who studied the outages. "There’s nothing you can point to that says it has all the hallmarks of an attack by a nation state. It could have been anybody."

Within the U.S. government, contingents have debated privately whether to acknowledge that the U.S. played no role in North Korea’s disruptions or remain silent to avoid detailed conversations about U.S. capabilities and policy on offensive cyber operations, which are considered highly classified.

The disclosure denying U.S. involvement was intended to convey how seriously the administration considers offensive cyberattacks, intended to be used only in the most serious cases and consistent with the State Department’s admonitions for foreign governments to always preserve access to the Internet for all citizens, one of the officials said.

Sony Pictures chief executive Michael Lynton told the AP in a new interview that he never knew whether the U.S. government electronically attacked North Korea as retaliation for the break-in at his company.

The government hinted earlier this year, on Jan. 2, that it wasn’t involved in the North Korea outages, but its intended message was too understated to be recognized as an outright denial. When the White House announced new economic sanctions against North Korea for what it called a "destructive and coercive cyberattack" against Sony, Obama spokesman Josh Earnest described the sanctions as "the first aspect of our response." In other words, the government was saying its initial response was coming 11 days after the mysterious attacks crippled North Korea’s networks.

As late as Thursday, Obama’s homeland security adviser, Lisa Monaco, declined to say whether the U.S. was behind the North Korea outages. Speaking at a cybersecurity conference in New York, Monaco would not answer a question from the U.S. attorney for the Southern District of New York, Preet Bharara, whether the administration was responsible and agreed it could be helpful to be ambiguous about the consequences of hacking American targets.

"I’m not going to comment, and I never would, on operational capabilities," she said. "But you want to be able to have a number of tools in your toolbox and reserve them for use."

FBI Assistant Director Joseph Demarest, head of the cyber division, added: "You have to be able to reserve some ability for your capabilities, your methods, in a way that protects that capability going forward."

At the time of the North Korea outages, the White House and the State Department also declined to say whether the U.S. government was

responsible. North Korea’s four principal connections to the Internet began having serious problems just hours after Obama blamed North Korea for hacking into Sony, which included disclosure of confidential company emails and business files and threats of terror attacks against U.S. movie theaters until Sony agreed to cancel the Christmas Day release of its film "The Interview." Sony eventually decided to release the profane comedy that pokes fun at North Korea leader Kim Jong Un and depicts an assassination plot against him, offering it online for $6 and in a relatively small number of theaters.

Obama promised Dec. 19 to retaliate against North Korea but pointedly did not indicate what he had planned: "We will respond proportionally," he said, "and we’ll respond in a place and time and manner that we choose. It’s not something that I will announce here today at a press conference." But Obama later described the Sony hacking as "an act of cyber vandalism," not an act of war.

As North Korea’s networks sputtered, on Dec. 22, State Department spokeswoman Marie Harf wouldn’t say whether U.S. fingerprints were involved, but her answer was widely interpreted as confirming a U.S. role: "As we implement our responses, some will be seen, some may not be seen."

One day later, Harf clarified. "I don’t think I actually winked or nudged," she said. "I said I can’t comment on those reports one way or the other. I can’t confirm them one way or the other. I don’t actually know that their Internet was out, and it’s not for me to speak to. I was broadly speaking about what the president has said but in no way was trying to link it to yesterday’s activity."

She added: "I understand it was sort of interpreted that way and did not mean to be."

FCC Signals Intent On Net Neutrality Decision, Redefines Broadband

After months of hemming and hawing, Federal Communications Commission Chairman Tom Wheeler indicated yesterday that he would advocate a net neutrality policy compatible with President Obama s vision for treating the Internet as a public utility and prohibit Internet service provider practices such as blocking, throttling, and paid prioritization.

"We re both pulling in the same direction," Wheeler said in a public interview at the Consumer Electronics Show in Las Vegas.

As recently as December, Wheeler appeared to be interested in a hybrid approach designed to accommodate the demands of infrastructure technology companies, which have vocally opposed the net neutrality framework Obama outlined in November. In Obama s view, consumer broadband should fall under Title II of the Telecommunications Act, which ensures that utilities like electricity are open to all and devoid of fast lanes.

Yesterday Wheeler dismissed the lobbying efforts of companies such as Cisco and IBM. "After the president said what he said about Title II, we still had a record bidding for spectrum from ISPs [Internet Service Providers] and continued announcements about new gigabit plants going out," he told interviewer Gary Shapiro, president of the Consumer Electronics Association.

Wheeler will introduce the final language for his proposed policy on February 5; FCC leaders will vote on the policy February 26.

In addition, Wheeler proposed changing the definition of broadband in order to promote faster internet speeds. Under the new standards, broadband, or "advanced telecommunications capability," in FCC parlance, would be defined as 25Mbps downstream and 3Mbps upstream an improvement from its current definition of 4Mbps downstream and 1Mbps upstream.

The recommendation stems from the FCC concern that internet service providers are failing to serve rural communities, which, in an increasingly digital economy, would effectively leave them cut off from trade and education.

According to the FCC, 55 million Americans lack access to broadband service that would meet the proposed redefinition. Of those, 53 million live in rural areas.

The FCC is required by Congress to determine whether broadband "is being deployed to all Americans in a reasonable and timely fashion." It last updated its broadband standards in 2010.

Google Researcher Reveals Zero-Day Windows 8.1 Vulnerability

A Google security researcher, ’James Forshaw’ has discovered a privilege escalation vulnerability in Windows 8.1 that could allow a hacker to modify contents or even to take over victims’ computers completely, leaving millions of users vulnerable.

The researcher also provided a Proof of Concept (PoC) program for the vulnerability. Forshaw says that he has tested the PoC only on an updated Windows 8.1 and that it is unclear whether earlier versions, specifically Windows 7, are vulnerable.

Forshaw unearthed the bug in September 2014 and thereby notified on the Google Security Research mailing list about the bug on 30th September. Now, after 90 days disclosure deadline the vulnerability and Proof of Concept program was made public on Wednesday.

The vulnerability resides in the function AhcVerifyAdminContext, an internal function and not a public API which actually checks whether the user is an administrator.

"This function has a vulnerability where it doesn’t correctly check the impersonation token of the caller to determine if the user is an administrator," Forshaw wrote in the mailing list. "It reads the caller’s impersonation token using PsReferenceImpersonationToken and then does a comparison between the user SID in the token to LocalSystem’s SID."

"It doesn’t check the impersonation level of the token so it’s possible to get an identify token on your thread from a local system process and bypass this check. For this purpose the PoC abuses the BITS service and COM to get the impersonation token but there are probably other ways."

The PoC contains two program files and some set of instructions for

executing the files which, if successful, finally result in the Windows calculator running as an Administrator. According to the researcher, the vulnerability is not in Windows User Account Control (UAC) itself, but UAC is used in part to demonstrate the bug.

Forshaw tested the PoC on Windows 8.1 update, both 32 bit and 64 bit versions, and he recommended users to run the PoC on 32 bit. To verify perform the following steps:

Put the AppCompatCache.exe and Testdll.dll on disk
Ensure that UAC is enabled, the current user is a split-token admin and the UAC setting is the default (no prompt for specific executables).
Execute AppCompatCache from the command prompt with the command line "AppCompatCache.exe c:\windows\system32\ComputerDefaults.exe testdll.dll".
If successful then the calculator should appear running as an administrator. If it doesn't work first time (and you get the ComputerDefaults program) re-run the exploit from 3, there seems to be a caching/timing issue sometimes on first run.
A Microsoft spokesperson confirms the vulnerability and says that it s already working on a fix:

"We are working to release a security update to address an Elevation of Privilege issue. It is important to note that for a would-be attacker to potentially exploit a system, they would first need to have valid logon credentials and be able to log on locally to a targeted machine. We encourage customers to keep their anti-virus software up to date, install all available Security Updates and enable the firewall on their computer."

At the time of posting this article, there's no patch available and all Windows 8.1 systems are vulnerable to hackers.

MIT Sites Defaced in Lead-up to Anniversary of Aaron Swartz's Death

The two year anniversary of the death of Aaron Swartz has been commemorated with an attack on the institution from which he siphoned documents.

Attackers going under the name of "Ulzr1z" defaced websites for courses at the Massachusetts Institute of Technology (MIT).

The attackers edited the homepages of 15 sites, replacing it with the text below, which has since been removed:

./ Hacked by Ulzr1z?Follow me @ulzr1z?#OpAaronSwartz?Hacked!

The attack affected MIT's Media Lab faculty, which hosts a number of course websites under its domain.

The attackers gained access to the WordPress admin panel, which controls all the websites, tweeting a screenshot to prove the access.

0x50776e6564 @ulzr1z ?Panel Admin Massachusetts Institute of Technology, #MIT #Hacked Acces to all other subdomain

The 15 defaced subdomains, including sites for courses on subjects such as Social Physics, were also posted on Pastebin.

This isn’t the first time that MIT’s suffered repercussions from the death of the internet activist, whose work included establishing the online gathering Demand Progress to campaign against the Stop Online Piracy Act (SOPA); co-authoring the web feed format RSS; and many other projects concerned with sociology, civic awareness and activism.

Two years ago, in 2013, attackers affiliating themselves with the Anonymous brand took down the school’s website to avenge Swartz’s death.

The website was also hijacked to host a personal tribute to Aaron Swartz that included tender comments from those who apparently knew the young man, who was only 24 when he was arrested.

The 2013 message was appended with an apologetic note to MIT’s web administrators, acknowledging that Anonymous didn’t directly blame MIT for the tragedy.

MIT runs the network from which, back in 2011, Swartz had acquired a trove of download-protected academic articles from the non-profit academic journal archive JSTOR, with the aim of republishing them without restriction.

Shortly following Swartz’s suicide, legislation that would have at least partly de-fanged the ferocity of the charges used against the internet activist was proposed.

Beyond Representative Zoe Lofgren’s so-called Aaron’s Law - which, as of August 2014, had been left to wither in a Congressional committee - the charges against Swartz have been dubbed "ridiculous and trumped up" by members of the House Judiciary Committee Representative.

Those Representatives have referred to Swartz as a "martyr" and, as of a year ago, were tasking an Oversight panel to look into the appropriateness of federal prosecutors’ actions against him.

Unfortunately, Saturday’s attack is similar to the ones launched previously, in that the main people who’ll suffer are the innocent bystanders who use the defaced sites - in this case, students.

Watch out! Macro-based Malware Is Making A Comeback

For the past several months, different groups of attackers have distributed malware through Microsoft Office documents that contain malicious macros, reviving a technique that has been out of style for over a decade.

Macros are scripts that contain commands for automating tasks in various applications. Microsoft Office programs like Word and Excel support macros written in Visual Basic for Applications (VBA) and these can be used for malicious activities like installing malware.

To prevent abuse, starting with Office XP, released in 2001, users are asked for permission before executing unsigned macros embedded in files, this being the primary reason why attackers have stopped using macros in favor of other malware distribution methods.

However, it seems that when coupled with social engineering the technique can still be effective and some cybercriminal groups have recently started to exploit that.

The Microsoft Malware Protection Center (MMPC) has recently seen an increasing number of threats using macros to spread their malicious code, malware researchers from Microsoft said in a blog post last Friday.

Two such threats that primarily target users in the U.S. and U.K. and whose activity peaked in mid-December are called Adnel and Tarbir. Both are distributed through macros embedded in .doc and .xls documents that are delivered via spam emails and typically masquerade as receipts, invoices, wire transfer confirmations, bills and shipping notices.

When opened, the documents provide victims with step-by-step instructions on how to enable the untrusted macros to run, the Microsoft researchers said. The combination of the instructional document, spam email with supposed monetary content, and a seemingly relevant file name, can be enough to convince an unsuspecting user to click the Enable Content button.

Another malware program that s being distributed through macros is called Dridex and targets online banking users. At their peak in November, the Dridex-related spam campaigns distributed up to 15,000 documents with malicious macros per day, according to researchers from security firm Trustwave.

The documents posed as invoices from software companies, online retailers, banking institutions and shipping companies and some of them had instructions on how to enable the macros to run, the Trustwave researchers said Tuesday via email.

It s not just cybercriminals who began using the macros technique again, but also state-sponsored attackers. Researchers Gadi Evron and Tillmann Werner recently presented their analysis of a cyberespionage operation dubbed Rocket Kitten at the Chaos Communication Congress in Hamburg. The attackers targeted government and academic organizations in Israel and Western Europe using spear-phishing emails that contained Excel files with malicious macros. When run, the macros installed a sophisticated backdoor.

Another cyberespionage campaign that used Word documents with malicious macros was CosmicDuke, which was uncovered in September and targeted at least one European Ministry of Foreign Affairs. It s heartwarming to see how kind the attackers are: when you open the email attachment, the Word document helps you enable macros by instructing you to click Enable Content , researchers from F-Secure said Wednesday in a blog post discussing connections between the CosmicDuke, MiniDuke and OnionDuke malware programs.

Japanese Newspaper Makes Bold Claim About Mt Gox’s Giant 2014 Bitcoin Loss

If you’re a Bitcoin user, you’ll know that 2014 was a bit of an annus horribilis for the "freedom currency."

Bitcoins are effectively cryptographic puzzles that are claimed by the

first person to solve each one, and thereafter traded at a value agreed between buyer and seller.

That makes them into a cash currency, more or less, but without any central backing or, for that matter, regulation.

There’s a good side to that: no government body can summarily devalue or disown your Bitcoin stash.

That can, and has, happened with centrally managed currencies, as for example in Zimbabwe in 2009.

Hyperinflation over a number of years rendered the Zimbabwe dollar so worthless that the government eventually disowned it altogether, leaving the economy to operate on other countries’ money, notably the US dollar and the South African Rand.

Effectively, the exchange rate against all other currencies officially became zero, so that any Zimdollars you had were quite literally worthless.

But no government, reserve bank or monetary authority can summarily wipe out your Bitcoins.

Of course, there’s a bad side to that: no regulator means that there are no regulatory protections, and no operating requirements for companies that offer to look after your Bitcoins for you.

In theory, you don’t need to entrust your Bitcoin holdings to anyone else, provided that you can find buyers who will accept them directly.

But that doesn’t give you a whole lot of liquidity you might be fiendishly rich in the Bitcoin world, yet unable to pay your rent, meet the loan repayments on your car, or even buy a loaf of bread.

So Bitcoin exchanges sprung up to act as an interface between the world’s official currencies and the world of Bitcoin.

Loosely speaking, you give someone some Bitcoins, and they let you at an agreed amount of regular money in return.

You might "deposit" BTC1, for example, and be given a balance of, say, $320 (the approximate rate on 2014-01-02) to spend in more familiar ways, or to transfer into a regular bank account.

In short, Bitcoin exchanges act much like banks, with deposits, withdrawals, balances and transaction records.

Yet they aren’t banks, any more than a retail store is a "bank" when it issues you a credit note for goods you’ve returned.

After all, Bitcoin isn’t really a currency, so, generally speaking, it’s not covered by any of the laws relating to currency trading, brokerage, banking and so on.

In other words, if the company to which you entrusted your precious Bitcoins suddenly tells you, "So sorry, they seem to have vanished," then, well, that’s that: you’re out of luck.

Indeed, the Bitcoin ecosystem has regularly suffered just that sort of

confidence-sapping announcement, though usually on a fairly modest scale, at least in global terms.

Examples prior to 2014 include:

May 2012. An exchange called Bitcoinica allegedly had $225,000 stolen, followed by another $90,000 later the same year.

September 2012. $250,000 was stolen from boutique exchange Bitfloor after an encryption lapse during a server upgrade.

November 2013. Small exchanges in Australia, China and Denmark "vanished along with the money" after claiming they'd heen hacked.

But in 2014, the Big Daddy of Bitcoin exchanges, Japan-based Mt. Gox, made a "So sorry, they seem to have vanished" announcement about a whopping 650,000 Bitcoins, worth approximately $800 each at the time.

The mystery of the missing BTCs was at first blamed on a cryptographic flaw in the Bitcoin protocol that Mt. Gox's coders hadn't defended against properly — something they really ought to have done, considering that they were sitting on half-a-billion dollars worth of other people's assets.

But that story didn't wash with everyone, not least those who thought that any abuse of the flaw concerned (it's euphemistically known as transaction malleability if you would like to look it up) ought to have been visible, albeit too late, in the transaction record.

? Greatly simplified, transaction malleability means that two transactions can be rigged to have the same supposedly-unique identifier. Crooked transactors can use a deliberately created duplicate-yet-different transaction pair to trick naive exchanges into thinking that something has gone wrong, and demand a refund. (Smart exchanges use additional checks to help repudiate bogus transaction repudiations.)

Some people suspected Mt. Gox insiders of simply taking the missing Bitcoins — or some of them, anyway — for themselves.

Ironically, the very sort of incautious attitude to coding that would make a transaction malleability exploit possible would probably also make it possible for rogue insiders to get away unnoticed with large-scale Bitcoin larceny.

That's where the story sat throughout the second half of 2014: something bad happened, but no-one quite knew whom to blame.

On New Year's Day, however, Japanese newspaper Yomiuri Shimbun dropped a bit of a bombshell.

It openly stated that there was "strong suspicion" that most of the missing Bitcoins were ripped off from inside.

Yomiuri Shimbun is claiming that the loss of about 7000BTC can be explained by cyberattack — in other words, crooks outside the company's network were the perpetrators — but that there is no evidence of cyberattack around the loss of the remaining 643,000BTC.

In short, 99% of the crime was an inside job.

Is that really what happened, do you think?

If so, is there a chance, however slim, that some of the missing funds might yet be recovered?

Zuckerberg: Facebook Will Protect Free Speech

In a show of solidarity with the victims of the attacks on French satirical newspaper Charlie Hebdo, Mark Zuckerberg pledged that extremism would not silence freedom of expression on Facebook.

In a post on his Facebook page, the co-founder and CEO of Facebook said the giant social network would uphold freedom of expression even when sharing content that some people might find offensive.

"I'm committed to building a service where you can speak freely without fear of violence," Zuckerberg wrote.

He recalled how an extremist in Parkistan fought to have him "sentenced to death" when Facebook refused to ban content about the Prophet Mohammed that offended the extremist.

"We stood up for this because different voices even if they're sometimes offensive can make the world a better and more interesting place," Zuckerberg wrote. "As I reflect on yesterday's attack and my own experience with extremism, this is what we all need to reject a group of extremists trying to silence the voices and opinions of everyone else around the world."

He ended the post with the hashtag #JeSuisCharlie.

A few years ago, an extremist in Pakistan fought to have me sentenced to death because Facebook refused to ban content about Mohammed that offended him.

We stood up for this because different voices - even if they're sometimes offensive - can make the world a better and more interesting place.

Facebook has always been a place where people across the world share their views and ideas. We follow the laws in each country, but we never let one country or group of people dictate what people can share across the world.

Yet as I reflect on yesterday's attack and my own experience with extremism, this is what we all need to reject - a group of extremists trying to silence the voices and opinions of everyone else around the world.

I won't let that happen on Facebook. I'm committed to building a service where you can speak freely without fear of violence.

My thoughts are with the victims, their families, the people of France and the people all over the world who choose to share their views and ideas, even when that takes courage. ?#?JeSuisCharlie?

58% of American Adults Are on Facebook

Facebook remains the most popular social media site in the United States. Fifty-eight percent of the entire adult population have an account, a study released Friday found.

Looking only at adults who use the Internet - 81% of all Americans - Facebook's numbers are much higher. Almost three-quarters of online adults used Facebook, the survey by the Pew Research Center found.

Facebook has become the baseline, "one stop shop" for online interaction, said Nicole Ellison, a professor of information science at the University of Michigan who's been studying the social media site for the past decade.

"If you look at any line in the post office and see what people are doing on their phones, they're frequently on Facebook," said Ellison, who helped design the Pew study.

"Facebook has become kind of a daily practice for many people," she said. "It's the default social site."

While the percentage of people using Facebook hasn't increased since 2013, the amount of time they spend of the site has. Fully 70% of users visit the site daily and 45% go several times a day, up from 63% who were daily visitors last year.

Facebook's latest conquest is older Americans. This year for the first time more than half of online adults over 65 were on Facebook 56% of them. That figure represents almost a third of all seniors nationwide.

They come on because their children encourage them. "Their children might say 'Mom, did you see the photos of the kids I posted on Facebook?' and that's when they get on," said Ellison.

Once there, seniors quickly find old friends, colleagues and school mates. "That has its own set of benefits in terms of combatting loneliness and creating social support," she said.

Despite Facebook's hegemony, Americans are also beginning to branch out. While not giving up their social space on Facebook, they're supplementing with second and third online hangouts, to reach other specific groups or do other things.
"We found that 52% of online adults were using two or more social media sites, compared to 42% the previous year - so 10% more had adopted another social media platform," Ellison said.

Among all U.S. adults, 23% use LinkedIn, 22% Pinterest, 21% Instagram and 19% Twitter, the survey found.

The photo-sharing platform Instagram skews younger. Fifty-three percent of people between 18 and 29 have an Instagram account. Almost half (49%) of all Instagrammers use the site daily.

Of Internet-using adults as a whole, 26% have an Instagram account.

Fifty percent of Internet users with college educations use LinkedIn, the business-oriented social networking group. In the online population as a whole, 28% have a LinkedIn account.

Pinterest, the hobby, craft and DIY site, is used predominantly by women. Twenty-eight percent of Internet users have an account. But 42% of American women who are online have an account while 13% of online men do, the Pew survey found.

The survey was conducted in September of 2014 by Princeton Survey Research Associates International for the Pew Research Center. It interviewed 2,003 Internet-using adults nationwide.

=~=~=~=